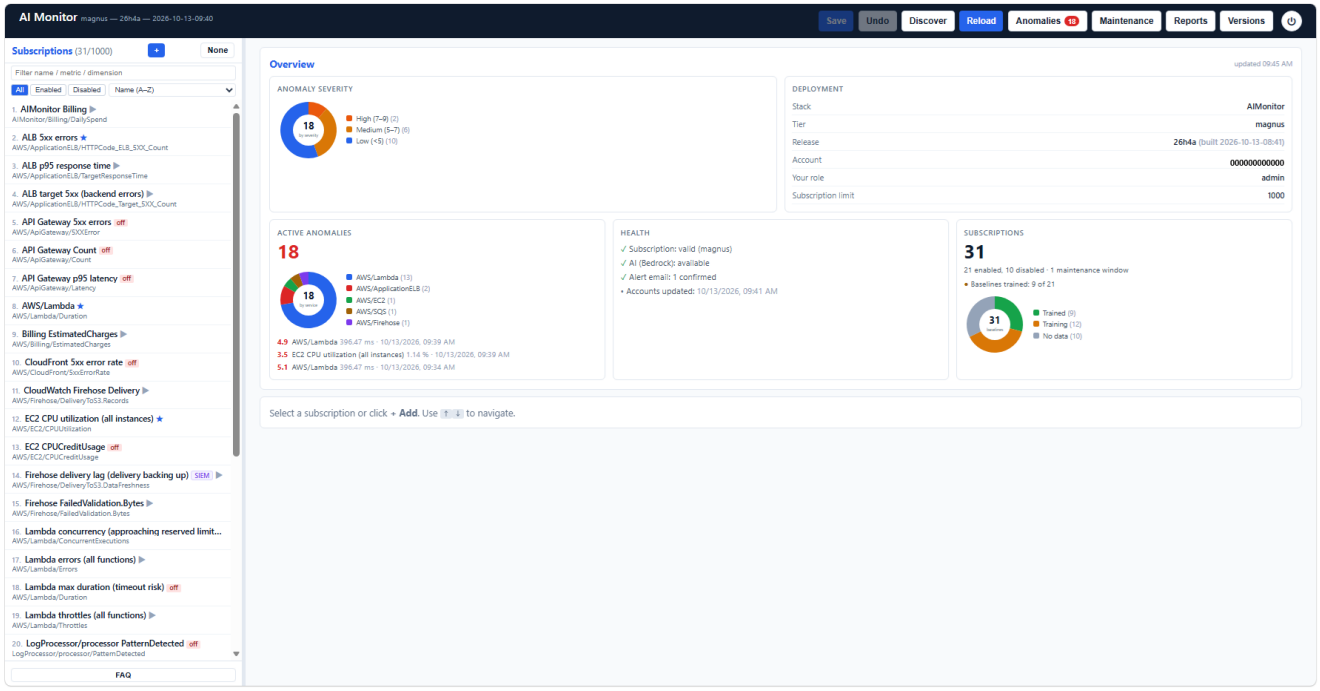
Subscription Editor Guide

Overview

The Subscription Editor is a built-in web UI for managing metric subscriptions, maintenance windows, anomaly review, reports, and AI-powered discovery. It is available on all tiers at:

https://<editor-domain>/editor

The editor is protected by Cognito authentication. On advanced+ tiers, RBAC is enforced via Cognito groups (admin = full access, viewer = read-only).



Note: A landing page has been provided with links to the editor and OpenSearch (https://<editor-domain>/).

Layout

- **Left panel:** Subscription list with status badges, trend indicators, and keyboard navigation (↑↓)
- **Right panel:** Edit form, anomaly viewer, maintenance windows, reports, or discovery wizard
- **Header:** Tier info, navigation buttons (Save, Undo, ✨ *Discover* Metrics, Reload, Anomalies, Maintenance, Reports, Versions, Logout)

Time zone: Set this in the FAQ page

Creating a Subscription

Discover Metrics

Click Discover to open the Discovery panel:

- **Active metrics:** Shows all CloudWatch metrics currently emitting data in your account (refreshed every 6h)
- **Catalog metrics:** Toggle "Show all AWS metrics" to see the full catalog (479 metrics across 57 namespaces)
- **Quick-start chips:** One-click templates for common monitoring patterns (Lambda errors, ALB 5xx, RDS CPU, etc.)
- **AI Suggest (advanced+):** Describe what you want to monitor in natural language. Press Enter or click ✨ Suggest. Bedrock returns a complete subscription configuration. Press Next for other suggestions, apply as needed navigating (Prev/Next).
- **Subscribe button:** Pre-fills the subscription form from the selected metric
- **Refresh ↻:** Triggers a synchronous discovery scan (~30s)

Manual

1. Click **+** in the left panel header
2. Fill in the required fields (Description, Namespace, Metric Name)
3. Configure dimensions, stat, period, threshold, and direction
4. Click **Save**

On save, the editor validates the configuration server-side and syncs the CloudWatch Metric Stream to include the new namespace.

Subscription Fields

Field	Description	Default
Description	Human-readable name (required, must be unique)	—
Namespace	CloudWatch namespace (e.g. AWS/Lambda, AWS/EC2)	—
Metric Name	The metric within the namespace. Clear and Preview to see all available.	—
Account ID	Blank = local only. * = all accounts. Or select specific accounts.	local
Enabled	Whether actively collecting and alerting	Yes
Stat	Aggregation: Average, Sum, Maximum, Minimum, SampleCount, p99/p95/p90	Average
Dimensions	JSON object. {} = all resources. Use ".*" for wildcard per-resource monitoring. Select from dropdown or type custom.	{}
Threshold	Z-score sensitivity (1.0–10.0). Lower = more sensitive. 3.0 catches top 0.3% outliers. Z-score alerting disabled when set to -1. Only "Alert if below" / "Alert if above" static thresholds will fire. Baseline still learns in the background.	3.0
Direction	**High** = only spikes. **Low** = only drops. **Both** = either.	Both
Tune	Those on advanced or above tiers will see ✨ Tune button, upon clicking AI will suggest some recommendations to tune the subscription (Ctrl+Click will leverage OpenSearch versus current anomalies).	—
Baseline (days)	Training period override. 0 = use tier default.	0
Period	Aggregation period: 60s, 5m, 15m, 1h	60s

Corr. Window	Minutes before/after anomaly to search Log Processor for errors	5
Log Pattern	When an anomaly fires, AI Monitor searches OpenSearch logs for entries matching selected Log Processor patterns within the correlation window.	—
Retention	Days to keep anomaly records. 0 = tier default. (advanced+)	0
Email	Send email alerts. "No (silent)" records anomalies without emailing.	Yes
Email threshold	Only email when score exceeds this. 0 = use anomaly threshold.	0
AI SIEM	When checked, this metric allows full kill-chain from Log Processor → AI Monitor → AI SIEM	
Runbook URL	Optional URL included in alert emails for quick incident response.	—
Alert if below*	Optional value that if triggered will alert.	—
Alert if above*	Optional value that if triggered will alert.	—

Alert if below/above*: AI Monitor anomaly detection doesn't recognize gradual changes, only sudden acceleration (runaway indexing, failed ILM policy, unexpected data growth). If you want to alert at an absolute threshold (e.g. <50GB free) breach specify values in this field.

Dimensions & Wildcards

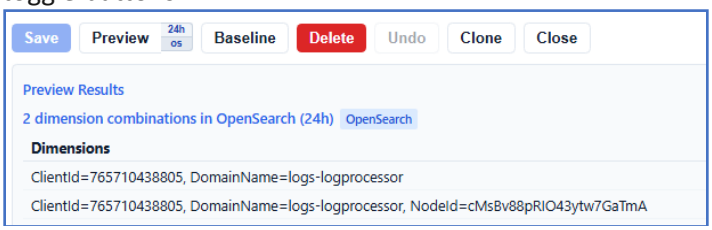
Dimensions control which specific resources are monitored:

- {} — Monitor the aggregate (all resources combined into one datapoint)
- {"FunctionName": "my-func"} — Monitor a specific resource
- {"FunctionName": ".*"} — Monitor each resource independently (wildcard). Each matching resource gets its own baseline.

Click the ✨ icon next to the dimensions field to wildcard all dimension keys.

Preview

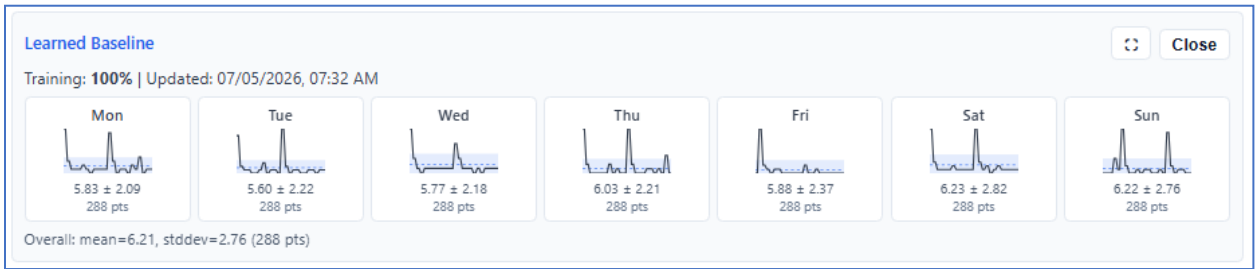
The **Preview** button fetches recent metric data to verify the subscription is configured correctly.
Use the Toggle between 1 hour and 24 hours and CloudWatch and OpenSearch using rightmost *Preview* toggle buttons:



When multiple dimension combinations exist, Preview shows a table with the values. The OpenSearch query includes an **Account** column showing which account the data came from. Right clicking on a specific dimension in the preview list displays a menu allowing you to create specific subscription for this resource, review/tweak make your changes and save.

Baseline Display

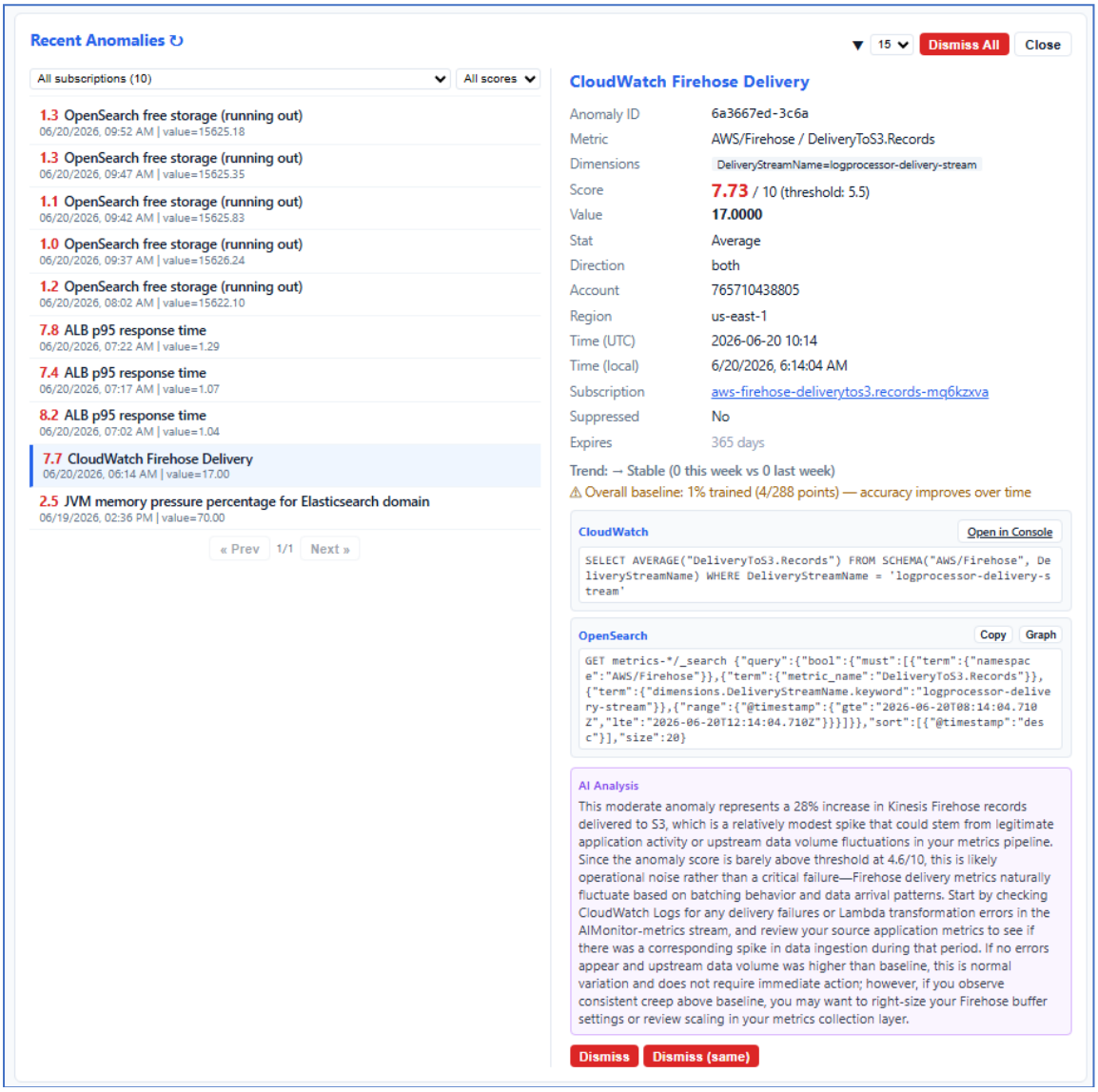
Click **Baseline** to view the learned behavior pattern. Shows a 7-column grid (Mon–Sun) with sparkline charts, mean±stddev bands, and training percentage. Hidden until training exceeds 50%.



Anomalies Panel

Click **Anomalies** in the header to view recent detections:

- Paginated list with score, description, timestamp, and score filter dropdown
- Detail panel: full metadata, dimensions, link to subscription, CloudWatch console deep link, Metrics Insights query, copy OpenSearch query, and Graph the OpenSearch sparkline
- AI Explanation (advanced+): natural language analysis of why the anomaly occurred
- Trend indicator: worsening/improving/stable/new
- Dismiss individual or all anomalies

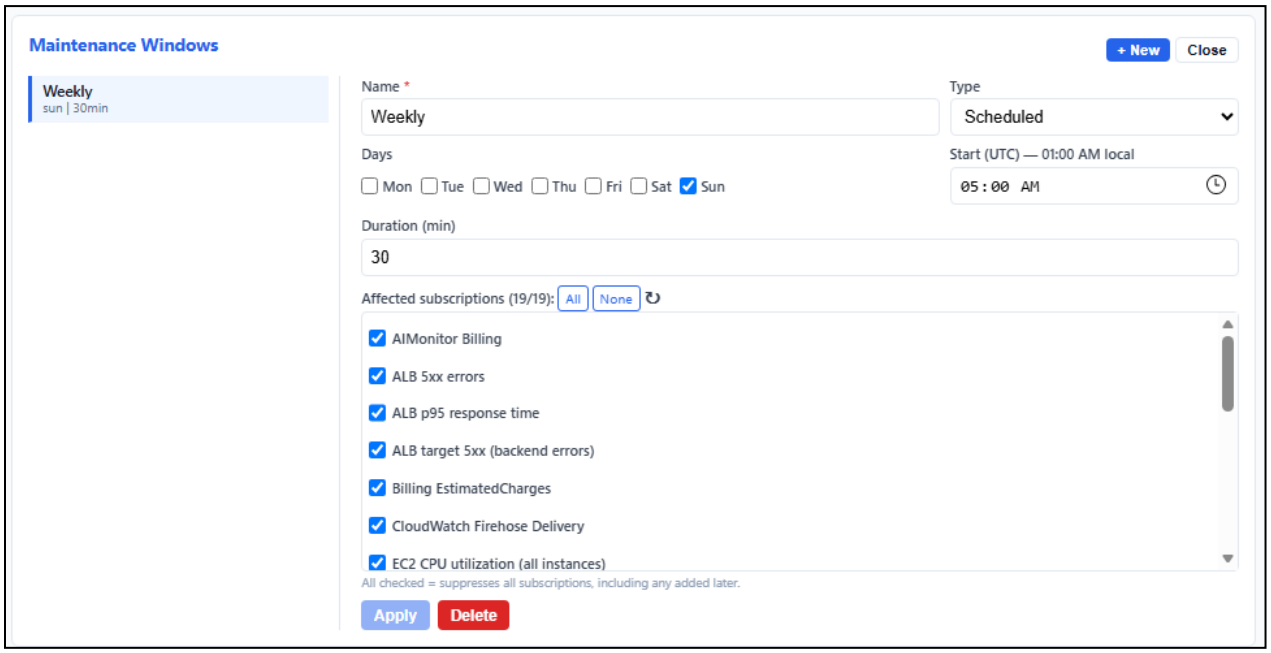


Note: The score filter dropdown also allows you manage dismissed anomalies. Dismissed anomalies are used for trending, they purge on their own.

Maintenance Windows

Click **Maintenance** to suppress alerts during known events:

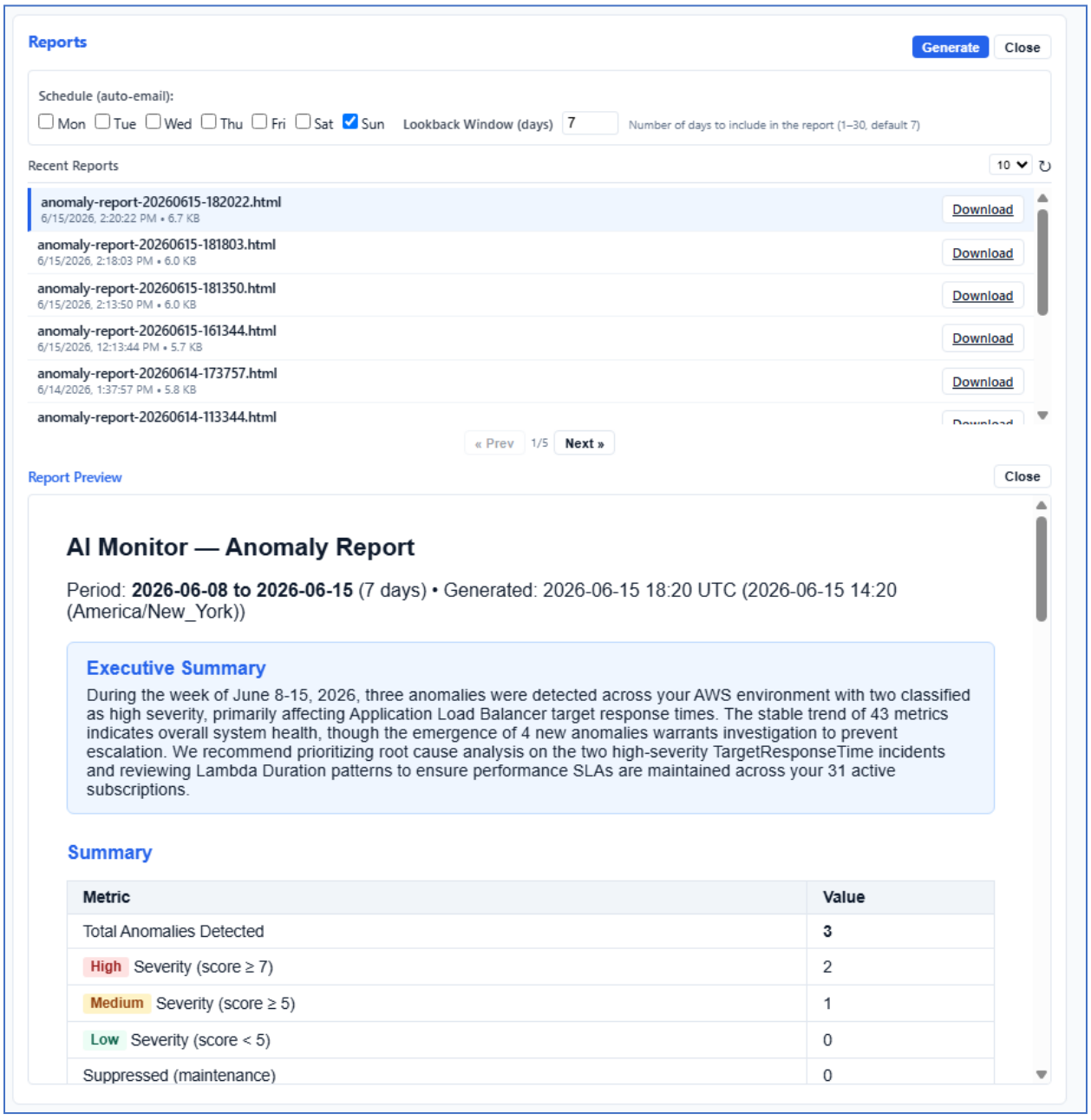
- **Scheduled:** Recurring on specific days/time (UTC) with duration
- **Ad-hoc:** Starts immediately for a set duration
- Select which subscriptions are affected (default: all)
- Active windows show a green **ACTIVE** badge



Reports

Click **Reports** to manage anomaly summary reports (advanced+):

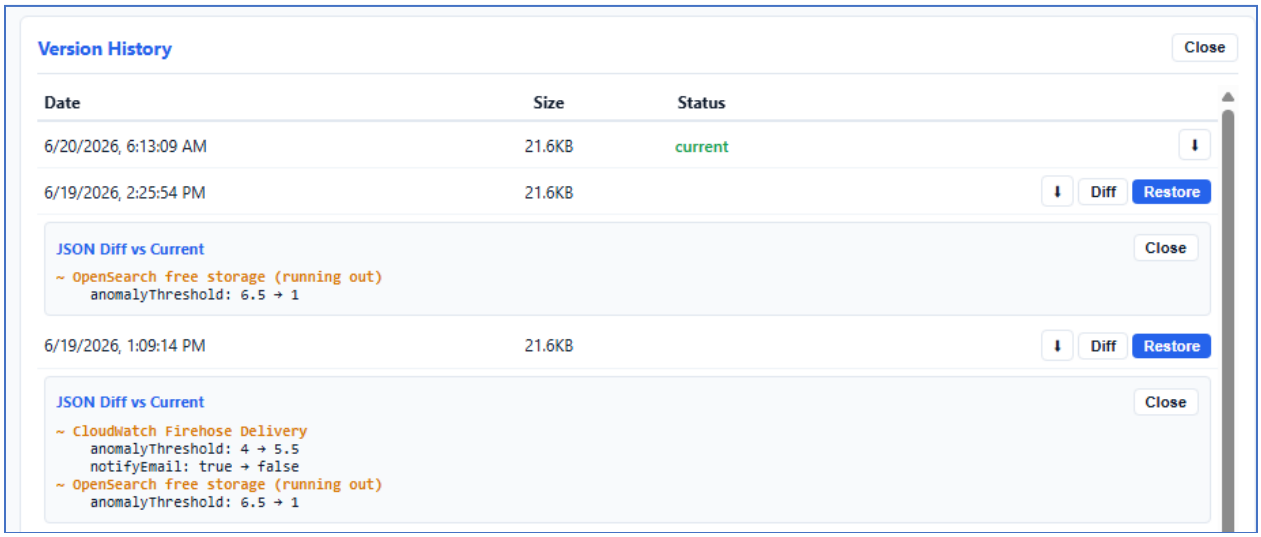
- **Generate:** Create an on-demand HTML report with cost analysis
- **Schedule:** Auto-email on selected days with configurable lookback window (1–30 days)
- Download or preview past reports inline



Version History

Click **Versions** to view the version history of your configuration:

- View timestamps, sizes, and current version indicator
- **Diff:** Compare any version against current
- **Restore:** One-click rollback to any previous version (admin only)
- **Download:** Export any version as JSON



Keyboard Shortcuts

Key	Context	Action
↑ ↓	Subscription list	Navigate subscriptions
↑ ↓	Anomaly list	Navigate anomalies (auto-pages)
↑ ↓	Maintenance list	Navigate windows
Double-click	Subscription list	Toggle enabled/disabled
Enter	AI prompt	Submit suggestion request

SNS Message Attributes

All anomaly alerts include SNS message attributes for filter-based routing:

Attribute	Type	Description
score	Number	Anomaly score (0–10)
severity	String	low / medium / high / critical
namespace	String	CloudWatch namespace
metricName	String	Metric name
subscriptionId	String	Subscription identifier
description	String	Subscription description
accountId	String	Source account ID

Use these to create SNS subscription filter policies for routing specific alerts to Slack, PagerDuty, Lambda, or other targets.

Tips

- Start with a high threshold (4.0–5.0) and lower it as the baseline matures
- Use **direction: high** for error metrics, **direction: low** for availability metrics
- Wildcard dimensions (".*") create independent baselines per resource — powerful but increases detection cycle time
- Use maintenance windows during deployments to avoid false positives
- The **Email threshold** field lets you record all anomalies but only email on high-severity ones
- Clone subscriptions to quickly set up similar monitoring with different thresholds or dimensions